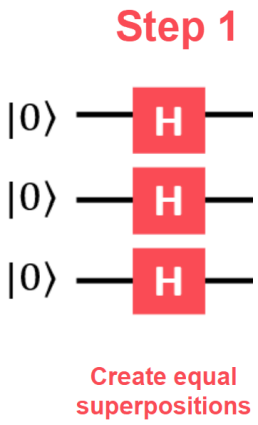
© 2023 The Coding School

Week 18: Summary of Key Concepts

Lecture

In lecture this week, we discussed various quantum search algorithms including Grover's algorithm.

1. **Unstructured search:** Grover's algorithm solves the unstructured search problem - the dataset we are searching through is not organized or sorted
2. **Grover's algorithm complexity: The Big-O complexity of Grover's algorithm is O($\sqrt{N}$).** This means that for the same size of database, Grover's provides a quadratic (square root of N) advantage over classical linear search.
3. **Grover's algorithm steps:** There are three steps to implementing Grover's algorithm:
    a. **Step 1: Creating a superposition**- **At the start of the search, we do not know where the state we are looking for is located**. Therefore, each of the quantum states is equally likely to be the right result. To express this idea, **we prepare an equal superposition of all the states by adding an H gate to each of the qubits** in the circuit as shown below:

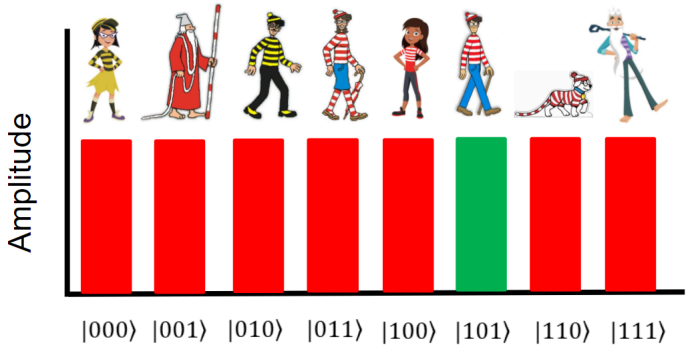


    i. **How many qubits do we need to use?** Remember that N qubits encode 2^N classical possibilities. **Therefore, for a database of size 2^N, you need to use N qubits.** For example, to search through 8 possibilities, you would use 3 qubits, to search through 128, you would use 7 qubits, and so on.

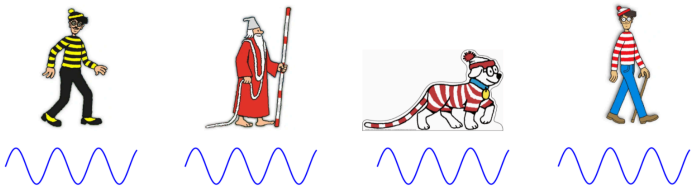
© 2023 The Coding School

ii. **Visualizing an equal superposition:** We can visualize this equal superposition state in two ways:

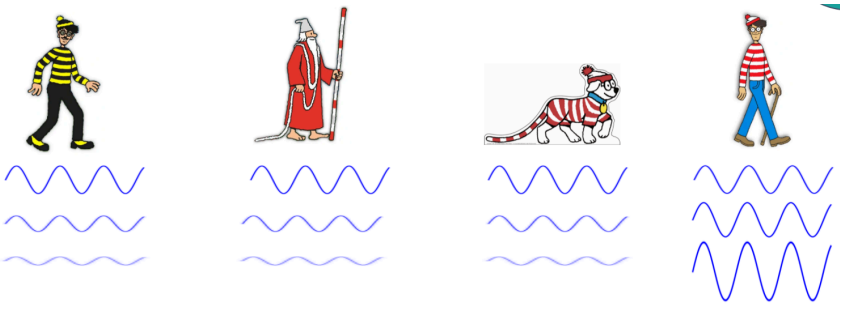
1. **Probability amplitudes:** The probability amplitudes of each of the possible answers is the same, as shown below:



2. **Wave-particle picture**: Using the fact that we can represent quantum states with waves, we can represent the initial state with waves of equal height (i.e. equal **amplitude**):



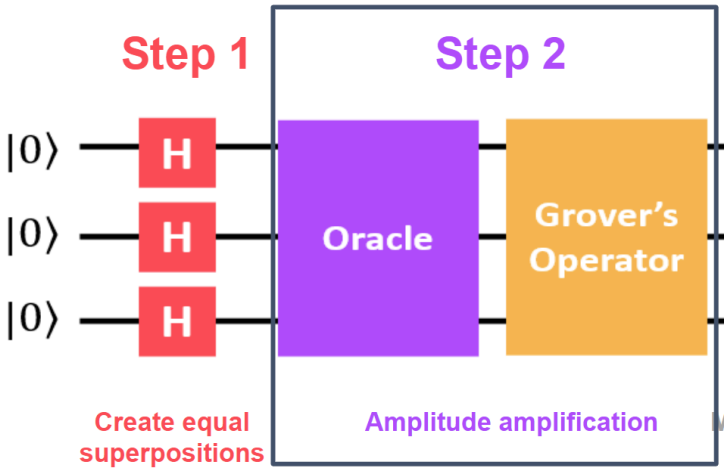
b. **Step 2: Amplitude Amplification- Amplitude amplification is the process of increasing the amplitude (and therefore the measurement probability) of the correct state and decreasing the amplitude of all other states through interference.** We can visualize amplitude amplification by considering the wave-particle picture of Grover search:



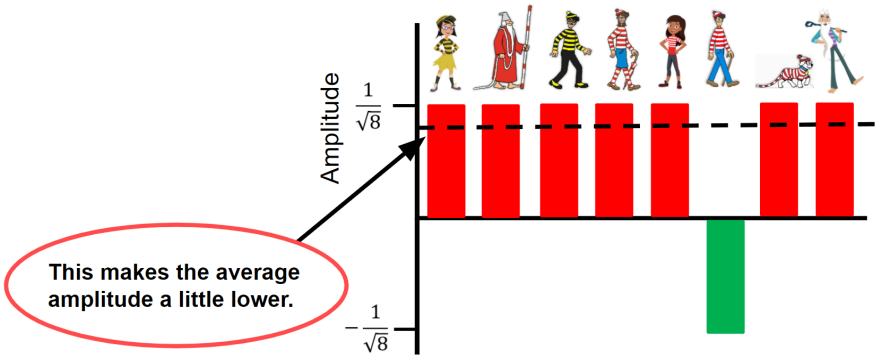
Here, each time we apply the algorithm, **the amplitudes (heights) of the incorrect states reduce, and the amplitude of the correct state increases**.

© 2023 The Coding School

We achieve amplitude amplification in two parts:

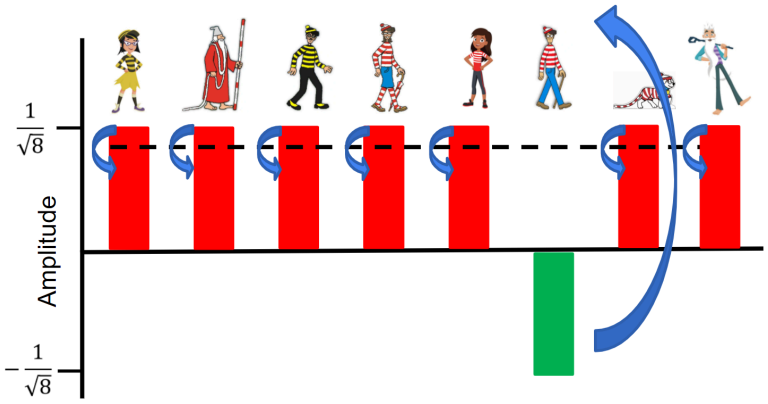


i. **Applying the oracle:** After creating an equal superposition, we first apply an oracle matrix to the circuit. **This matrix flips the sign of the state we are searching for, leaving all the other states unaffected.** This operation slightly reduces the average of the amplitudes of all the states. This operation can be visualized as shown in the probability amplitude graph below (the average is depicted by the dotted black line)

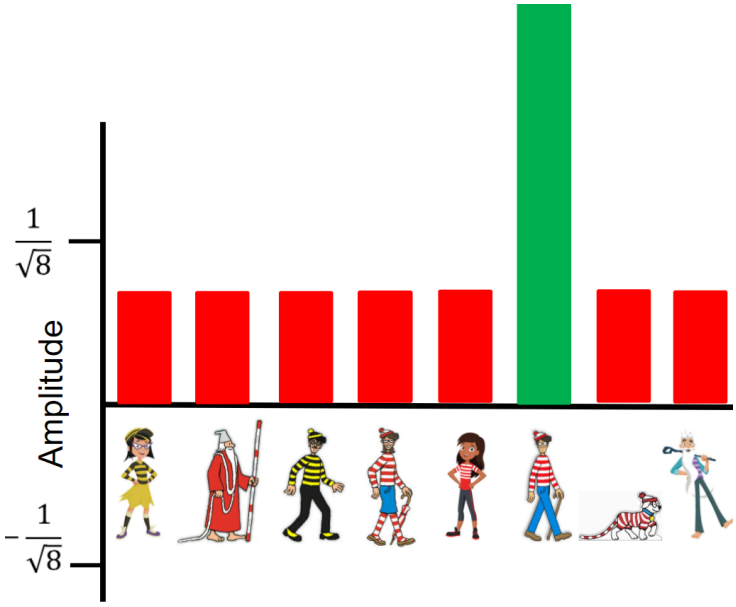


ii. **Applying Grover's operator:** After applying the oracle, we apply Grover's operator (also called the diffusion operator). This operator reflects all the states about the average of the amplitudes of all the states, as shown in the image below:

© 2023 The Coding School



The end result of this operator is that the amplitude of the correct state is much higher than that of all the other states, as shown below:



With this step, we have achieved amplitude amplification! The amplitude of the right state is higher than all the other states. Step 2 gets repeated multiple times to keep on amplifying the amplitude of the right state. **The optimal number of times Step 2 needs to be repeated is approximately** $\sqrt{N}$ - this number of iterations maximizes the amplitude of the correct state. **Therefore, the complexity of Grover's algorithm is O($\sqrt{N}$)**

© 2023 The Coding School

c. **Step 3: Measurement** - At the end of the algorithm, after applying Step 2 the optimal number of times, we make a measurement, and, with a very high probability, measure the right state!

4. **Current Status of Grover's**: Although it has been shown theoretically that Grover's algorithm offers a benefit over classical linear search, **our current quantum computers are not powerful enough to demonstrate this advantage practically**. We will need quantum computers with thousands of fault-tolerant qubits to demonstrate the advantage of Grover's algorithm. This is why Grover's is classified as a long-term algorithm.

Lab

In lab this week, we implemented Grover's search by using Qiskit's built-in Grover function.

1. **Algorithm-level coding -** In the past, when we implemented quantum protocols, we built up the circuit gate-by-gate. This is known as **gate-level coding**, and is a great way to first learn quantum circuits. However, as we tackle more complicated quantum protocols and algorithms, gate-level coding cannot keep up with the increasing number of gates required to build the circuits needed. Therefore, quantum programming languages offer libraries that automatically implement the circuits for different protocols and algorithms. As users, we just have to define the size of the problem, the problem inputs, and the algorithm we want to use to solve the problem. This level of coding, where we worry about the algorithm being used (or the application being developed) is known as **algorithm or application-level coding.**
2. **Qiskit's Grover function:** Qiskit's Grover function, which we used in lab this week, is an example of algorithm-level coding - we specify the size of the Grover problem and the state we are searching for, and the Grover function creates the circuit and solves the problem for us.

Further readings and resources:

- Qiskit textbook page on Grover's Algorithm

© 2023 The Coding School

  - URL: https://qiskit.org/textbook/ch-algorithms/grover.html
- Grover's Algorithm original paper
  - URL: https://arxiv.org/pdf/quant-ph/9605043.pdf
- Azure Quantum on Grover's Algorithm
  - URL: https://docs.microsoft.com/en-us/azure/quantum/concepts-grovers